IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA

RAVEN RICHARDSON, *individually and on behalf of all others similarly situated,* Plaintiff, v. **ADVANCE STORES COMPANY, INCORPORATED, ADVANCE AUTO PARTS, INC., and SNOWFLAKE INC.,** Defendants.	**Civil Action No. 5:24-cv-488** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Raven Richardson ("Plaintiff") brings this Class Action Complaint, individually and on behalf of all others similarly situated (the "Class Members"), against Defendants Advance Stores Company, Incorporated, Advance Auto Parts, Inc., and Snowflake Inc. (collectively, "Defendants"), and alleges as follows, based upon information and belief, investigation of counsel, and the personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach where unauthorized third-party criminals retrieved and exfiltrated highly sensitive data belonging to Plaintiff and millions of Class Members, as a result of Defendants' failure to reasonably and adequately secure this highly sensitive consumer data (the "Data Breach") and failure to adequately implement, and ensure third-party vendors implemented, reasonable cybersecurity protocols.

2. The Data Breach involved a targeted cyberattack against Defendant Snowflake Inc. ("Snowflake"), a major player in the data storage and analysis industry, as well as several of Snowflake's corporate clients, including Defendants Advance Stores Company, Incorporated and

Advance Auto Parts, Inc. (together, "Advance Auto Parts"). The Data Breach resulted in the theft of extensive consumer data—affecting more than half a *billion* individuals—and was of such a significant scale that it spurred a Congressional investigation into the breach.

3. Snowflake is a cloud-based data hosting company used by some of the biggest and most recognized companies in America and overseas, including Ticketmaster, AT&T, LendingTree, and Advance Auto Parts. Headquartered in Bozeman, Montana, Snowflake reportedly controls roughly 20% of the web hosting market share globally.

4. Advance Auto Parts is a leading automotive aftermarket parts provider serving both professional installers and do-it-yourself customers.[1]

5. Advance Auto Parts stores customer data in a virtual warehouse or "Data Cloud" provided by Defendant Snowflake (the "Advance Auto Parts Snowflake Data Cloud").

6. On June 14, 2024, Advance Auto Parts filed a Form 8-K with the United States Securities and Exchange Commission announcing: "On May 23, 2024, Advance Auto Parts, Inc. (the 'Company') identified unauthorized activity within a third-party cloud database environment containing Company data and launched an investigation with industry-leading experts. On June 4, 2024, a criminal threat actor offered what it alleged to be Company data for sale. The Company has notified law enforcement."[2] The "third-party cloud database environment" belonged to Defendant Snowflake.

7. In July 2024, Advance Auto Parts began sending Notices of Data Breach to impacted individuals, including Plaintiff and Class Members. These Notices confirmed that the personally identifying information (PII or "Private Information") implicated in the Data Breach

[1] *Advance Auto Parts, Inc. – Our Story*, Advance Auto Parts, https://corp.advanceautoparts.com/our-story/default.aspx (last accessed Aug. 20, 2024).
[2] Advance Auto Parts, Inc., SEC Form 8-K (May 23, 2024), https://www.sec.gov/Archives/edgar/data/1158449/000115844924000162/aap-20240523.htm.

included Social Security numbers, driver's license or other government issued identification numbers, and dates of birth.[3] According to public reports, the Data Breach exposed the PII of 2.3 million individuals whose data was collected by Advance Auto Parts as part of the company's job application process.[4]

8. Mandiant, an Alphabet-owned cybersecurity firm that assisted Snowflake in the aftermath of the Data Breach, identified the threat actor responsible for infiltrating Snowflake's inadequately secured networks and systems as "UNC5537"—a hacking entity with members based in Turkey and North America. Reportedly, the cybercriminal group used info-stealing malware to grab credentials for companies' Snowflake accounts and then easily logged into any accounts that did not have two-factor authentication enabled—a security feature that is a norm in the industry and which Snowflake easily could have required of all employee and customer accounts. Instead, however, the security feature was turned off by default on Snowflake accounts.[5]

9. According to the June 2024 Snowflake Data Breach report by Mandiant, the stolen data is already being leaked and sold on the dark web for the purpose of the cybercriminals' financial gain: "UNC5537 is systematically compromising Snowflake customer instances using stolen customer credentials, advertising victim data for sale on cybercrime forums, and attempting to extort many of the victims."[6]

10. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols, consistent with industry standards, and necessary to protect Plaintiff's and Class Members' PII from the foreseeable threat of a

[3] *See* Plaintiff Richardson Notice of Security Incident, **Exhibit A**.
[4] Matt Kapko, *Snowflake-linked attack on Advance Auto Parts exposes 2.3 million people*, CybersecurityDive (July 15, 2024), https://www.cybersecuritydive.com/news/advance-auto-parts-snowflake-data-breach/721353/.
[5] Lily Hay Newman, *The Sweeping Danger of the AT&T Phone Records Breach*, WIRED (July 12, 2024), https://www.wired.com/story/att-phone-records-breach-110-million/.
[6] *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, MANDIANT (June 10, 2024), https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion.

cyberattack. This included Defendants' failure to employ and enforce Multi-Factor Authentication (MFA).

11. MFA is a simple yet robust security system that requires more than one method of authentication from independent categories of credentials (i.e., a username/password and confirmation link sent via email). Industry experts have described MFA as a "critical component in protecting against identity theft and specifically against attacks related to the successful theft of passwords."[7]

12. Although MFA is an industry standard, both Snowflake and Advance Auto Parts failed to enforce MFA—indeed the ability to enforce MFA is a feature which was unavailable to the administrators of the Advance Auto Parts Snowflake Data Cloud. Despite the unavailability of this feature, Advance Auto Parts still elected to use Snowflake's Data Cloud.

13. In the aftermath of the Data Breach, the threat actors boasted to journalists that the Data Breach was enabled by Snowflake's lack of MFA enforcement.[8] Because Snowflake left the option to enable MFA up to individual users, data environments could easily be compromised through weak links — users who elect to not enroll in MFA for their accounts.[9]

14. Snowflake, as a data cloud service provider, is and was at all relevant times aware that failing to implement and enforce MFA requirements could lead to substantial loss of sensitive information.

15. Advance Auto Parts and its data security employees were on notice that they, as administrators of the Advance Auto Parts Snowflake Data Cloud, were unable to enforce MFA.

---

[7] Shane Snider, *Snowflake's Lack of MFA Control Leaves Companies Vulnerable, Experts Say*, InformationWeek (June 5, 2024), https://www.informationweek.com/cyber-resilience/snowflake-s-lack-of-mfa-control-leaves-companies-vulnerable-experts-say.
[8] *Id.*
[10] *Id.*

16. Defendants failed to take necessary actions to ensure the safety of customers' and employees' PII, knowing they had designed and/or were using flawed systems vulnerable to breach. Accordingly, Defendants shirked their duties to protect customers' and employees' information from unauthorized access.

17. In light of recent high profile cyberattacks targeting companies that house large troves of sensitive data, like Snowflake and Advance Auto Parts, it was highly foreseeable that Defendants would be the target of a cyberattack.

18. Despite their duties under the law to Plaintiff and Class Members to protect and safeguard their Private Information, and the foreseeability of a data breach, Defendants failed to implement reasonable and adequate data security measures, which directly resulted in the Data Breach.

19. Defendants owed a non-delegable duty to Plaintiff and Class Members to implement reasonable and adequate security measures to protect their Private Information and to oversee third parties entrusted with that data to ensure those third parties had proper data security measures in place. Yet, Defendants maintained and/or shared Plaintiff's and Class Members' Private Information in a negligent and/or reckless manner.

20. Plaintiff's and Class Members' Private Information was compromised due to Defendants' negligent and/or reckless acts and omissions and Defendants' repeated failures to reasonably and adequately protect Plaintiff's and Class Members' Private Information.

21. Now armed with the Private Information accessed in the Data Breach, cybercriminals can use or sell the Private Information to further harm Plaintiff and Class Members in a variety of ways, including: destroying their credit by opening new financial accounts and taking out loans in Class Members' names; using Class Members' names to improperly obtain

medical services; using Class Members' Private Information to target other phishing and hacking intrusions; using Class Members' Private Information to obtain government benefits; and otherwise assuming Class Members' identities. In fact, as noted above, leading cybersecurity firm Mandiant has found that the threat actors responsible for the Data Breach are *already* advertising victim data for sale on cybercrime forums.[10] Likewise, the Form 8-K filed by Advance Auto Parts with the SEC noted that "[o]n June 4, 2024, a criminal threat actor offered what it alleged to be [Advance Auto Parts] data for sale."[11]

22. As a result of the Data Breach, Plaintiff and Class Members face a substantial risk of imminent harm relating to the exposure and misuse of their Private Information. Plaintiff and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

23. Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

24. Accordingly, Plaintiff brings this action against Defendants, seeking redress for Defendants' unlawful conduct and asserting claims for: (i) negligence and negligence *per se*; (ii) breach of implied contract; (iii) unjust enrichment; (iv) bailment; and (v) breach of fiduciary duty.

25. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including reasonable and adequate improvements

[10] *Id.*
[11] Advance Auto Parts, Inc., SEC Form 8-K (May 23, 2024), https://www.sec.gov/Archives/edgar/data/1158449/000115844924000162/aap-20240523.htm.

to Defendants' data security systems, policies, and practices, the implementation of annual audits reviewing the same, adequate credit monitoring services funded by Defendants, and payment for the costs of repairing damaged credit as a result of the Data Breach.

THE PARTIES

26. Plaintiff Raven Richardson is a natural person, resident, and citizen of the State of Mississippi. Plaintiff Richardson applied to work at Advance Auto Parts.

27. Defendant Advance Auto Parts, Inc. is a Virginia corporation with its principal place of business located at 4200 Six Forks Road, Raleigh, NC 27609.

28. Defendant Advance Stores Company, Incorporated is a Virginia corporation with its principal place of business located at 4200 Six Forks Road, Raleigh, NC 27609 and is a wholly-owned subsidiary of Advance Auto Parts, Inc.

29. Defendant Snowflake Inc. is a Delaware corporation with its headquarters and principal place of business located at 106 East Babcock Street, Suite 3A, Bozeman, MT 59715.

JURISDICTION AND VENUE

30. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, including Plaintiff, as defined below, is a citizen of a different state than Defendants, there are more than 100 putative Class Members, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

31. This Court has general personal jurisdiction over the Advance Auto Parts Defendants because their principal places of business are in this District.

32. This Court has personal jurisdiction over Defendant Snowflake because Defendant Snowflake is authorized to conduct business in this District and has entered into contracts to conduct substantial business in this District, including with the Advance Auto Parts Defendants.

Defendant Snowflake has engaged in continuous, systematic, and substantial activities within this State, including substantial marketing and sales of services and products in connection with the Data Breach within this State. Further, a substantial part of the acts and omissions giving rise to Plaintiff's claims against all Defendants occurred in and emanated from this District.

33. Venue is proper under 18 U.S.C § 1391 because this is the District in which the Advance Auto Parts Defendants have the most significant contacts—and it is the Advance Auto Parts Defendants' current and former job applicants and employees which make up the Class of injured individuals bringing this action. Venue is proper under 18 U.S.C § 1391(b)(2) because a substantial part of the acts and omissions giving rise to Plaintiff's claims, including those against Advance Auto Parts, occurred in and emanated from this District.

DEFENDANTS' BUSINESSES

34. Advance Auto Parts is a leading automotive aftermarket parts provider that serves both professional installer and do-it-yourself customers. Advance Auto Parts employs individuals who work at Advance Auto Parts stores across the country, including across the State of North Carolina.

35. Snowflake is a cloud-based data storage and analytics company that provides a single platform for data storage, processing, and analysis. Snowflake advertises security across its products and services, promising "secure collaboration" and marketing itself as "the AI data cloud for cybersecurity."[12]

36. Plaintiff and Class Members are former or current employees or job applicants of Advance Auto Parts. Sources suggest that as many as 2.3 million current and former Advance

[12] *Industry Solutions*, Snowflake, https://www.snowflake.com/en/ (last accessed Aug. 20, 2024); *Cybersecurity*, Snowflake, https://www.snowflake.com/en/solutions/departments/cybersecurity/ (last accessed Aug. 20, 2024).

Auto Parts employees and applicants were impacted in the Data Breach.[13]

37. In the regular course of their business, Defendants solicit, receive, create, handle, and transfer consumers' Private Information. Indeed, to apply for a job or work as an employee with Advance Auto Parts, Plaintiff and Class Members were required to provide highly sensitive Private Information and entrust Advance Auto Parts to properly secure that highly sensitive information, including some or all of the following:

- Full names and addresses;
- Personal email addresses and phone numbers;
- Information related to credit and debit card numbers, bank account statements and financial account details;
- Dates of birth;
- Social Security numbers; and
- Government-issued identification.

38. This sort of Private Information is extremely sensitive and is extremely valuable to criminals because it can be used to commit serious identity theft crimes.

39. When entrusting Advance Auto Parts with their Private Information during the job application process, job seekers and employees reasonably expected that Advance Auto Parts would keep their information confidential and securely maintained, use that information for business purposes only, and make only authorized disclosures of that information.

40. Advance Auto Parts acknowledges the importance of Plaintiff's and Class Members' Private Information, stating in the Privacy Policy posted on its website: "We seek to

[13] Matt Kapko, *Snowflake-linked attack on Advance Auto Parts exposes 2.3 million people*, CybersecurityDive (July 15, 2024), https://www.cybersecuritydive.com/news/advance-auto-parts-snowflake-data-breach/721353/.

use reasonable organizational, technical, and administrative measures to protect Personal Information within our organization."[14] In the case of the instant Data Breach, however, Advance Auto Parts failed to keep Plaintiff's and Class Members' Private Information safe.

41. Snowflake is one of the largest data storage providers in the United States and contracts with thousands of companies worldwide to securely store consumer and employee data on its Snowflake Data Cloud. As such, Snowflake is responsible for developing and maintaining environments which collect and process personal data for hundreds of millions of Americans—and advertises that it does so securely. Posted on the "Security Hub" page of Snowflake's webpage is a promotional quote from Snowflake's Chief Information Security Officer and VP of Information Security, Brad Jones: "Since our founding in 2012, the security of our customers' data has been our highest priority. This unwavering commitment is why we're continuously strengthening our industry-leading, built-in security policies to deliver a trusted experience for our customers."[15]

42. Upon information and belief, Defendants promise to, among other things: keep Private Information private; comply with industry standards related to data security and Private Information, including FTC guidelines; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Plaintiff and Class Members obtain from Defendants, directly or indirectly, and provide adequate notice to individuals if their Private Information is disclosed without authorization.

43. However, Defendants did not maintain adequate security to protect their systems

[14] *Privacy Policy*, Advance Auto Parts, https://shop.advanceautoparts.com/o/privacy-notice (last accessed Aug. 20, 2024).
[15] *Snowflake Security Hub*, Snowflake, https://www.snowflake.com/en/resources/learn/snowflake-security-hub/ (last accessed Aug. 20, 2024).

from infiltration by cybercriminals or adequately implement, or ensure third-party vendors implemented, reasonable cybersecurity protocols.

44. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties owed to Plaintiff and Class Members and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

45. Yet, contrary to Defendants' representations, Defendants failed to implement adequate data security measures, including adequate oversight of third parties entrusted with highly sensitive consumer PII, as evidenced by Defendants' admission of the Data Breach, which affects, to date, millions of individuals.

The Data Breach of Advance Auto Parts Systems and Networks

46. Upon information and belief, Advance Auto Parts uses Snowflake's data cloud services to store the Private Information entrusted to it by job applicants and employees.

47. In a June 14, 2024 Form 8-K filed with the SEC, Advance Auto Parts confirmed that the Data Breach occurred.

48. Nearly one month later, in mid-July 2024, Advance Auto Parts began notifying impacted individuals like Plaintiff and Class Members.

49. In the Notice of Data Breach sent to Plaintiff and Class Members, Advance Auto Parts wrote:

> **What Happened**
> On May 23, 2024, we learned that, like many other companies, an unauthorized third party gained access to certain information maintained by Advance Auto Parts within Snowflake, our cloud storage and data warehousing vendor. We began an investigation to determine the nature and scope of the incident with the support of third-party experts and took measures to contain the incident and terminate the unauthorized access, Our investigation determined

> that an unauthorized third party accessed or copied certain information maintained by Advance Auto Parts from April 14, 2024 to May 24, 2024. We conducted a detailed review and analysis of the affected information to determine the types of information contained therein and to whom the information relates. This review was completed on June 10, 2024.
>
> **What Information Was Involved**.
> The personal information about you involved in this incident may include your name and the following: Social Security number, driver's license or other government issued identification number, and date of birth. This information was collected as part of the Advance Auto Parts job application process.[16]

50. Omitted from the Notice of Data Breach is information explaining the root cause of the Data Breach, the vulnerabilities exploited by the cybercriminals, and Defendants' plans for data breach remediation to ensure similar breaches do not continue to occur and expose customers' Private Information. To date, these omitted details have not been explained or revealed to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches.

51. Upon information and belief, the cybercriminal group UNC5537 specifically targeted Defendant Snowflake based on its status as a major cloud-based data storage provider and Advance Auto Parts based on their status as a major American corporation with enormous amounts of valuable Private Information—including the Private Information of Plaintiff and Class Members.

52. Plaintiff further believes her and Class Members' Private Information has been or soon will be disseminated on the dark web, to be available for purchase, because that is the *modus operandi* of cybercriminals, and a detailed report by cybersecurity expert Mandiant found that UNC5537 is "advertising victim data for sale on cybercrime forums, and attempting to extort many

[16] Plaintiff Richardson Notice of Security Incident, **Exhibit A**.

of the victims."[17] Furthermore, in the Form 8-K filed by Advance Auto Parts with the SEC, it acknowledged: "On June 4, 2024, a criminal threat actor offered what it alleged to be [Advance Auto Parts] data for sale."

53. The targeted attack was a foreseeable risk which Defendants were aware of and knew they had a duty to guard against. It is well-known that entities, such as Defendants, which collect and store confidential and sensitive Private Information of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity.

54. The Data Breach was a targeted cyberattack expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of consumers, like Plaintiff and Class Members.

Advance Auto Parts' Breached Data was Hosted on Snowflake's Data Cloud

55. The Data Breach occurred, in part, because Advance Auto Parts failed to adequately supervise third-party vendors with which it entrusted the highly sensitive Private Information of its customers, job applicants, and employees. Public reports confirmed that "[t]he threat actors had unauthorized access to Advance [Auto Part]'s Snowflake cloud environment, a cloud storage and data warehousing vendor, for more than a month prior to the June 10 discovery."[18]

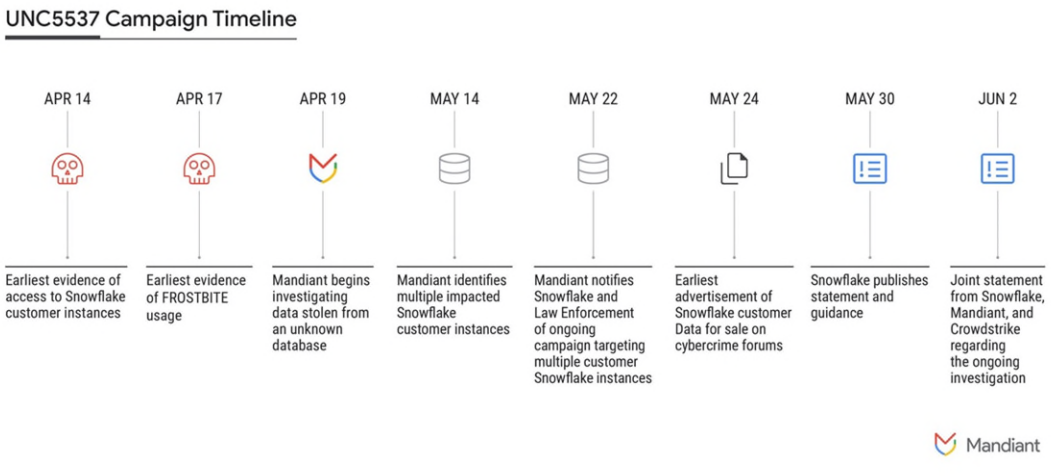
56. Snowflake provides digital warehouses, known as "Snowflake Data Clouds" for its thousands of clients around the world, and as a result has access to, stores, and maintains huge

[17] *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, MANDIANT (June 10, 2024), https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion.
[18] *Advance Auto Parts Data Breach Affects 2.3M Customers*, Dark Reading (July 11, 2024), https://www.darkreading.com/cyberattacks-data-breaches/advance-auto-parts-data-breach-affects-2m-customers.

datasets of sensitive Private Information belonging to its corporate clients' customers and employees. Snowflake's corporate clients include Advance Auto Parts and many others, including AT&T, LendingTree, and Live Nation/Ticketmaster.

57. In April 2024, an unauthorized party, suspected to be affiliated with the cybercriminal group UNC5547, gained access to at least 165 Snowflake customer accounts, stealing consumer data from Advance Auto Parts, Live Nation, Ticketmaster, AT&T, Santander, and LendingTree/QuoteWizard, among others.

58. Google-owned cybersecurity incident response firm, Mandiant, which Snowflake retained to help it investigate the incident, attributed the breach to UNC5537 and identified April 14, 2024 as the "earliest evidence of access to Snowflake customer instances."[19]



20

59. Mandiant describes the hackers as "financially motivated" and as comprised of members in North America and at least one member in Turkey.[21]

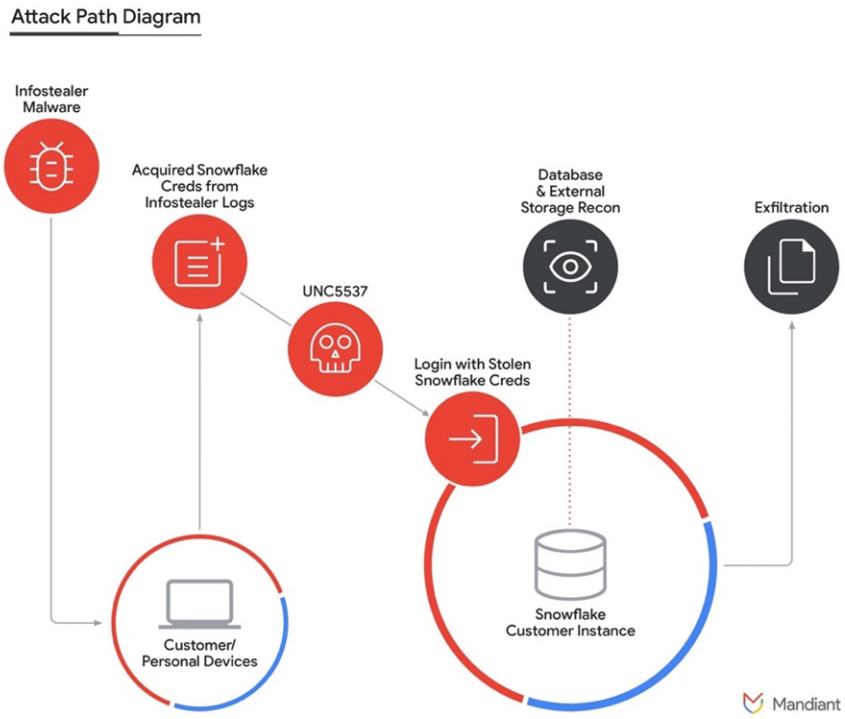
60. Data belonging to Snowflake's corporate clients has already been published on

[19] *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, MANDIANT (June 10, 2024), https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion.
[20] *Id.*
[21] *Id.*

known cybercrime forums, and is being advertised as "for sale."[22]

Mandiant Confirms That Failure to Implement Multi-Factor Authentication Was a Significant Underlying Cause of the Data Breach

61. In a June 2024 report on the Data Breach published by Mandiant, Mandiant explained that the Data Breach was largely the culmination of a failure by Snowflake to require that its accounts use multi-factor authentication, noting: "the impacted accounts were not configured with multi-factor authentication enabled, meaning successful authentication only required a valid username and password."[23]



[24]

62. Multi-factor authentication (or MFA) is a simple yet robust security system that requires more than one method of authentication from independent categories of credentials (e.g., a username/password and confirmation link sent via email).

[22] *Id.*
[23] *Id.*
[24] *Id.*

63. It is industry standard to have MFA administrator enforcement on an application level, instead of leaving it up to every user to decide whether they want to enroll with MFA or not, according to Ofer Maor, cofounder and Chief Technology Officer of data security investigation firm Mitiga. Maor notes that "MFA is a critical component in protecting against identity theft, and specifically against attacks related to the successful theft of passwords through phishing, malware (infostealers), or leakage of reused passwords from compromised sites."[25] Jon Sternstein of Stern Security explained that while Snowflake does let administrators see if staff has MFA enabled, "[i]t is surprising that the built-in account management within Snowflake doesn't have more robust capabilities like the ability to enforce MFA … While it's odd that MFA cannot be enforced on Snowflake, the companies should also understand how their teams are using applications and ensure that it's done securely."[26]

64. Because the responsibility to enforce MFA was shared by Snowflake and its corporate clients, including Advance Auto Parts, Snowflake cannot rest blame for the Data Breach solely on its clients, who did not require MFA to secure their Snowflake accounts. This is because Snowflake also could have, but did not, require its clients to use MFA. Indeed, the security feature requiring multi-factor authentication was tu*rned off by default* on Snowflake accounts.[27] At the same time, Advance Auto Parts knew (or their IT professionals were on notice) that they were unable to enforce MFA on the Advance Auto Parts Snowflake Data Cloud, and yet they elected to use Snowflake's services despite that critical flaw. Accordingly, the Data Breach was the product of a joint failure by Snowflake and Advance Auto Parts to implement the most basic

[25] Shane Snider, *Snowflake's Lack of MFA Control Leaves Companies Vulnerable, Experts Say*, InformationWeek (June 5, 2024), https://www.informationweek.com/cyber-resilience/snowflake-s-lack-of-mfa-control-leaves-companies-vulnerable-experts-say.
[26] *Id.*
[27] Lily Hay Newman, *The Sweeping Danger of the AT&T Phone Records Breach*, WIRED (July 12, 2024), https://www.wired.com/story/att-phone-records-breach-110-million/.

cybersecurity feature: enabling and/or enforcing MFA.

65. Snowflake, as a major data cloud service provider, is aware that certain basic security measures are critical to protecting sensitive information, include implementing MFA requirements that include enforcing MFA on all accounts. Indeed, Snowflake recently signed the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") "Secure By Design" pledge, which explains that "what it means to be secure by design" is that "[o]ut-of-the-box, products should be secure with additional security features such as multi-factor authentication (MFA)."[28] In a press release announcing its signing of CISA's pledge, Snowflake wrote: "MFA is one of the most important security measures that every business needs to utilize, and when paired with network policies, it delivers comprehensive security."[29]

66. Yet neither Snowflake nor Advance Auto Parts took any measures to ensure that the sensitive information located on Snowflake's cloud was fully protected by ensuring and enforcing MFA on all user accounts. This failure left Snowflake's customers' database instances vulnerable to infiltration by malicious actors. As Mandiant explained: "The threat actor used [ ] stolen credentials to access the customer's Snowflake instance and ultimately exfiltrate valuable data. *At the time of the compromise, the account did not have multi-factor authentication (MFA) enabled*."[30]

67. By implementing a policy to enable MFA by default, or by going further to enforce MFA from the top-down design of Snowflake or within the Advance Auto Parts database instance, this Data Breach could have been avoided entirely.

---

[28] *Secure by Design*, CISA, https://www.cisa.gov/securebydesign (last accessed Aug. 20, 2024); *Snowflake Advances Cybersecurity Excellence by Joining CISA Secure by Design Pledge*, Snowflake: Blog (July 29, 2024), https://www.snowflake.com/en/blog/snowflake-cybersecurity-cisa-secure-by-design/.
[29] *Snowflake Advances Cybersecurity Excellence by Joining CISA Secure by Design Pledge*, Snowflake: Blog (July 29, 2024), https://www.snowflake.com/en/blog/snowflake-cybersecurity-cisa-secure-by-design/.
[30] *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, MANDIANT (June 10, 2024), https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion.

68. In the months following the Data Breach, Snowflake made significant changes to its MFA policies and practices, including: "developing a plan to require our customers to implement advanced security controls, like multi-factor authentication (MFA) or network policies, especially for privileged Snowflake customer accounts" and "continuing to strongly engage with our customers to help guide them to enable MFA and other security controls as a critical step in protecting their business."[31] By July 2024, Snowflake's VP of Information Security, Brad Jones, announced that Snowflake had been "working on product capabilities that allow Snowflake admins to make multifactor authentication (MFA) mandatory and monitor compliance with this new policy."[32]

69. Defendants had obligations created by the FTC, contract, industry standards, and common law to keep its customers' and former customers', as well as their beneficiaries', Private Information confidential and protected from unauthorized access and disclosure.

70. Plaintiff and Class Members entrusted Defendants with their Private Information, either directly or indirectly, with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

71. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew, or should have known, they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

72. Due to Defendants' inadequate security measures, failure to adequately train their

[31] *CISO Corner*, SNOWFLAKE, https://www.snowflake.com/en/resources/learn/snowflake-security-hub/ (last accessed Aug. 20, 2024).
[32] *Id.*

employees on reasonable cybersecurity protocols, and their delayed notice to victims, Plaintiff and Class Members face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

Defendants' Failure to Comply with FTC Guidelines

73. The Federal Trade Commission ("FTC") has regularly promulgated guidelines for businesses, which highlight the necessity of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

74. For example, in 2016, the FTC updated its published guidelines, *Protecting Personal Information: A Guide for Business*, which laid out standard and accepted cyber-security measures for businesses to implement to protect consumers' private data. The guidelines advise businesses, *inter alia*, to: encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[33]

75. The FTC's guidelines further advise businesses: not to maintain PII longer than necessary for authorization of a transaction; to limit access to sensitive data; to require complex passwords to be used on networks; to use industry-tested methods for security; to monitor for suspicious activity on the network; and to verify that third-party service providers have implemented reasonable security measures.[34]

76. To underscore the binding significance of the promulgated guidance, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further identify the measures businesses *must* take to

[33] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[34] *Id.*

meet their data security obligations consistent with federal law.

77. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to its clients', or its clients' customers', Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

78. Defendants were at all times fully aware of their obligations to protect the Private Information of consumers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants' Failure to Comply with Accepted Industry Standards for Data Security

79. In light of the evident threat of cyberattacks seeking consumers' Private Information, several best practices have been identified by regulatory agencies and experts that, at a minimum, should be implemented by corporations like Defendants who deal with millions of consumers' data, including but not limited to: educating and training all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; monitoring and limiting network ports; protecting web browsers and email management systems; and limiting which employees can access sensitive data.

80. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

81. These foregoing frameworks are existing and applicable industry standards, and

Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendants' Failure to Adequately and Reasonably Secure Plaintiff's and Class Members' Private Information Increased Their Risk of Fraud and Identity Theft

82. Cyberattacks and data breaches like the Data Breach are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

83. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[35]

84. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identify thieves who desire to extort and harass victims and take over victims' identities to engage in illegal financial transactions under the victims' names. As noted above, the cybersecurity firm Mandiant found that victim data stolen in the Data Breach has already been advertised "for sale on cybercrime forums."[36]

85. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique known as "social engineering" to obtain even more

[35] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf.

[36] MANDIANT, UNC5537 TARGETS SNOWFLAKE CUSTOMER INSTANCES FOR DATA THEFT AND EXTORTION, (June 10, 2024) https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion.

information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

86. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[37]

87. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[38]

88. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

89. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

90. According to the GAO, which conducted a study regarding data breaches:

---

[37] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last visited Dec. 11, 2023).

[38] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
>
> GAO Report at 29.

91. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

92. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts, or the accounts of deceased individuals for whom Class Members are the executors or surviving spouses, for many years to come.

93. Private Information can sell for as much as $363 per record according to the Infosec Institute.[39] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

94. For this reason, Defendants knew or should have known about these dangers and strengthened their data handling systems as well as their training of employees in cybersecurity protocols accordingly. Defendants were on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendants failed to properly prepare for that risk.

[39] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

Defendants' Failure to Adequately and Reasonably Protect Against The Data Breach was Reckless and Negligent

95. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and/or failed to implement adequate data security oversight and practices necessary to safeguard stored Private Information. Altogether, Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to implement best practices around multi-factor authentication;

c. Failing to adequately protect consumers' Private Information;

d. Failing to properly monitor their own data security systems for existing intrusions;

e. Failing to train employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to oversee third-party vendors entrusted with consumers' Private Information;

g. Failing to train all staff members on the policies and procedures with respect to Private Information as necessary and appropriate for staff members to carry out their functions and to maintain the security of Private Information;

h. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

i. Failing to adhere to industry standards for cybersecurity as discussed above;

and

j. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

96. Defendants negligently, recklessly, and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Defendants' computer network and systems which contained unsecured and unencrypted Private Information, upon information and belief, for multiple days.

97. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

Plaintiff's and Class Members' Damages

98. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Defendants have done nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered.

99. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach, which is now in the hands of cybercriminals.

100. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to time with her family, work and/or recreation.

101. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

102. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

103. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

104. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

105. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

106. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiff's and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

107. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

108. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in similar cases.

109. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

110. Plaintiff and Class Members have suffered or will suffer actual injury as a direct

result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security numbers, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

111. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

112. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

113. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiff's Experiences

Plaintiff Richardson's Experience

114. Plaintiff Richardson applied to work at Advance Auto Parts which required that she provide Advance Auto Parts with her sensitive Private Information, including her full name, address, Social Security number, government-issued identification, date of birth, and other personal information.

115. Advance Auto Parts obtained, stored, and maintained Plaintiff Richardson's and Class Members' Private Information, including on the cloud platform provided and maintained by Defendant Snowflake. Collectively, Defendants owe Plaintiff Richardson a legal duty and obligation to protect her Private Information from unauthorized access and disclosure.

116. Advance Auto Parts notified Plaintiff Richardson on July 10, 2024, nearly two months after it had discovered the Data Breach, and nearly three months after it initially occurred, that her Private Information was compromised in the Data Breach and disclosed as a result of Defendants' inadequate data security practices.

117. Defendants have yet to confirm the specific information that was compromised in the Data Breach. However, on information and belief, the compromised data includes Plaintiff Richardson's name, contact information (such as email address and home address), Social Security number, date of birth, and government-issued identification.

118. Plaintiff Richardson is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the

documents. Plaintiff Richardson has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Richardson diligently chooses unique usernames and passwords for her various online accounts.

119. As a result of the Data Breach, Plaintiff Richardson made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit.

120. Plaintiff Richardson has been forced to spend multiple hours attempting to mitigate the effects of the Data Breach. She will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to time with her family, work and/or recreation. This is time that is lost forever and cannot be recaptured.

121. Plaintiff Richardson suffered actual injury and damages as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of her Private Information, a form of intangible property that Defendants obtained from Plaintiff Richardson; (b) violation of her privacy rights; (c) the theft of her Private Information; (d) loss of time; (e) imminent and impending injury arising from the increased risk of identity theft and fraud; (f) failure to receive the benefit of her bargain; and (g) nominal and statutory damages.

122. Plaintiff Richardson has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud.

123. As a result of the Data Breach, Plaintiff Richardson anticipates spending

considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Richardson will continue to be at a present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

124. Plaintiff Richardson has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

125. Plaintiff brings this action against Defendants individually and on behalf of all other persons similarly situated.

126. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **National Class: All persons or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Defendants identified as being among those individuals whose Private Information was compromised in the Data Breach (the "Class").**

127. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

128. Plaintiff reserves the right to amend or modify the Class definition or create additional subclasses as this case progresses.

129. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. As of July 2024, public reports claim that as many as 2.3 million Advance Auto Parts employees and/or former job applicants may be affected.

130. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable and adequate security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

d. Whether Defendants owed a duty to Plaintiff and Class Members to safeguard their Private Information;

e. Whether Defendants breached their duty to Plaintiff and Class Members to safeguard their Private Information;

f. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g. Whether Defendants should have discovered the Data Breach sooner;

h. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

i. Whether Defendants' conduct was negligent;

j. Whether Defendants breached implied contracts with Plaintiff and Class Members;

k. Whether Defendants were unjustly enriched by unlawfully retaining a benefit

conferred upon them by Plaintiff and Class Members;

l. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

131. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

132. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

133. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the data of Plaintiff and Class Members was stored on the same network and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

134. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to

individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

135. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a classwide basis.

136. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants' security measures and workforce training protocols to protect its data systems were reasonable and adequate in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

137. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to names and addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Advance Auto Parts.

CLAIMS FOR RELIEF

COUNT I
Negligence and Negligence Per Se
(*On Behalf of Plaintiff and the Class*)

138. Plaintiff re-alleges and incorporates by reference factual allegations above as if fully set forth herein.

139. By collecting and storing the Private Information of Plaintiff and Class Members, in their computer systems and networks, and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer systems and networks—and Class Members' Private Information held within—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

140. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

141. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of individuals that Defendants were aware, or should have been aware, could be injured by

inadequate data security measures.

142. Defendants' duty of care to use reasonable and adequate security measures and to adequately train their workforces in reasonable data security protocols arose as a result of the special relationship that existed between Defendants and consumers, which is recognized by laws and regulations including but not limited to the FTC Act and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

143. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

144. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

145. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain reasonable and adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of its and/or its third-party vendors' networks and systems;

c. Failing to ensure that their email systems had reasonable data security

safeguards in place;

d. Failing to have in place reasonable and adequate mitigation policies and procedures;

e. Failing to enable and/or enforce the use of multi-factor authentication;

f. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;

g. Failing to detect in a timely manner that Plaintiff's and Class Members' Private Information had been compromised; and

h. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

146. Plaintiff and Class Members have no ability to protect their Private Information that was or remains in Defendants' possession.

147. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches amongst companies responsible for storing vast troves of consumer data, like Defendants.

148. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in one or more types of injuries to Plaintiff and Class Members.

149. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information, and

failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

150. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

151. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

152. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

153. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

154. Plaintiff re-alleges and incorporates by reference factual allegations above as if fully set forth herein.

155. Defendants acquired and maintained the Private Information of Plaintiff and the Class that they received either directly, or which Snowflake received indirectly via Advance Auto Parts.

156. When Plaintiff and Class Members provided their Private Information to Advance Auto Parts for the purpose of obtaining employment, they entered into implied contracts with Advance Auto Parts and its affiliates, such as Snowflake.

157. Plaintiff and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

158. Defendants directly solicited, offered, and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

159. Defendants accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services and products to Plaintiff and Class Members.

160. In accepting such information and payment for services and products, Defendants entered into implied contracts with Plaintiff and Class Members whereby Defendants became obligated to reasonably safeguard Plaintiff's and Class Members' Private Information.

161. In delivering their Private Information to Defendants, Plaintiff and Class Members intended and understood that Defendants would adequately safeguard the data.

162. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

163. The implied promises include but are not limited to: (1) taking steps to ensure that any workforce members who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the

control of their workforce members is restricted and limited to achieve an authorized purpose; (3) restricting access to qualified and trained workforce members; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) requiring and/or enforcing multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

164. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

165. Had Defendants disclosed to Plaintiff and Class Members that they did not have adequate data security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to Defendants.

166. Defendants recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and Class Members.

167. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

168. Defendants breached the implied contracts with Plaintiff and Class Members by failing to take reasonable and adequate measures to safeguard their Private Information as described herein.

169. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

170. Plaintiff re-alleges and incorporates by reference all factual allegations above as if fully set forth herein.

171. This count is pleaded in the alternative to the breach of contract claims (Count II).

172. Upon information and belief, Defendants fund any data security measures they implement entirely from their general revenues, including from money they make based upon representations of protecting Plaintiff's and Class Members' Private Information.

173. There is a direct nexus between money paid to Defendants and the requirement that Defendants keep Plaintiff's and Class Members' Private Information confidential and protected.

174. Plaintiff and Class Members paid Defendants a certain sum of money, or a certain sum of money was paid on their behalf, which was used to fund any data security measures implemented by Defendants.

175. As such, a portion of the payments made by or on behalf of Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

176. Protecting the Private Information of Plaintiff and Class Members is integral to Defendants' businesses. Without their data, Defendants would be unable to provide goods and services, including the auto parts services and related employment and database cloud services that comprise Defendants' core businesses.

177. Plaintiff's and Class Members' data and Private Information has monetary value.

178. Plaintiff and Class Members directly conferred a monetary benefit on Defendants by purchasing goods and/or services from Defendants, directly or indirectly, and/or by supplying

Defendants, directly or indirectly, with their Private Information in the process of applying for employment, which has value, from which value Defendants derive their business value, and which should have been protected with adequate data security.

179. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

180. Defendants enriched themselves by saving the costs they reasonably should have expended on adequate data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable and adequate level of security that would have prevented the Data Breach, Defendants instead chose to shirk their data security obligations to increase profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective data security measures. Plaintiff and Class Members suffered as a direct and proximate result of Defendants' calculated failures to provide the requisite reasonable and adequate data security.

181. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement reasonable and adequate data management and security measures that are mandated by federal law and industry standards.

182. Defendants acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

183. If Plaintiff and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants.

184. Plaintiff and Class Members have no adequate remedy at law.

185. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in its continued possession; (vii) loss of privacy from the authorized access and exfiltration of their Private Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

186. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

187. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

COUNT IV
Bailment
(*On Behalf of Plaintiff and the Class*)

188. Plaintiff re-alleges and incorporates by reference all factual allegations above as if fully set forth herein.

189. Plaintiff and Class Members provided Private Information to Defendants, which Defendants were under a duty to keep private and confidential.

190. Plaintiff's and Class Members' Private Information is personal property and was conveyed to Defendants for the certain purpose of keeping the information private and confidential.

191. Plaintiff's and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendants were aware of the risks they took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

192. Once Defendants accepted Plaintiff's and Class Members' Private Information, they were in the exclusive possession of that information, and neither Plaintiff nor Class Members could control that information once it was within the possession, custody, and control of Defendants.

193. Defendants did not safeguard Plaintiff's or Class Members' Private Information when they failed to adopt and implement reasonable and adequate data security safeguards to prevent the known risk of a cyberattack.

194. Defendants also did not safeguard Plaintiff's or Class Members' Private Information when they maintained Plaintiff's or Class Members' Private Information for years and years after the initial transactions occurred.

195. Defendants' failure to safeguard Plaintiff's and Class Members' Private

Information resulted in that information being accessed or obtained by third-party cybercriminals.

196. As a result of Defendants' failure to keep Plaintiff's and Class Members' Private Information secure, Plaintiff and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

197. Plaintiff re-alleges and incorporates by reference all factual allegations above as if fully set forth herein.

198. In light of the special relationship between Defendants and Plaintiff and Class Members, Defendants became fiduciaries by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members: (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information Defendants store (and where).

199. Defendants had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship to keep their Private Information secure.

200. Defendants breached their fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

201. Defendants breached their fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

202. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i)

actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendants' services they received.

203. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class Action and appointing Plaintiff as Class Representative and her counsel as Class Counsel;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendants to utilize appropriate methods and

policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, nominal damages, and/or statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: August 26, 2024

Respectfully submitted,

/s/ *David M. Wilkerson*
David M. Wilkerson
THE VAN WINKLE LAW FIRM
11 N. Market Street
Asheville, NC 28801
(828) 258-2991
dwilkerson@vwlawfirm.com

James J. Pizzirusso*
HAUSFELD LLP
888 16th Street, N.W., Suite 300
Washington, D.C. 20006
(202) 540-7200
jpizzirusso@hausfeld.com

Steven M. Nathan*
HAUSFELD LLP
33 Whitehall Street, Fourteenth Floor
New York, NY 10004
(646) 357-1100
snathan@hausfeld.com

Counsel for Plaintiff

****Pro Hac Vice Forthcoming***